SUBJECT: Data Classification and Protection	Effective Date 8-27-2015	Policy Number 4-008.1	
	Supersedes 4-008	Page 1	Of 6
	Responsible Authority Vice Provost for Information Technologies & Resources		

APPLICABILITY/ACCOUNTABILITY

This policy applies to all employees of the University of Central Florida who maintain or use university data. This includes all full-time and part-time employees, adjuncts and others on temporary or time-limited appointments, all volunteers and courtesy appointees, student workers, and all persons paid by or through the university such as contractors, consultants, or employees of direct support organizations.

POLICY STATEMENT

Data are critical assets of the university. All members of the university community have a responsibility to protect the confidentiality, integrity, and availability of data generated, accessed, modified, transmitted, stored, or used by the university, irrespective of the medium on which the data resides, such as electronic, paper, or other physical form, or the means by which the data may be transmitted such as email, text message, facsimile or other means. It is the policy of the University of Central Florida to classify types of data in use at the university and to provide the appropriate levels of information security and protection.

Individuals working for or on behalf of the university who create, view, or manage university data are responsible for implementing appropriate managerial, operational, physical, and technical controls for access to, use of, transmission of, storage of, and disposal of university data in compliance with this policy. The UCF information security officer must be notified immediately if data classified as highly restricted or restricted is, or is suspected to have been, lost or disclosed to unauthorized parties, or if any unauthorized use of university information systems is occurring or is suspected to have occurred. In the event of a suspected information security incident, users should take no action to delete any data or attempt to investigate.

Any violation of this policy and procedures may result in immediate loss of network and computer access privileges, seizure of equipment, loss of research laboratory access, or removal of inappropriate information posted on university-owned computers or university-supported Internet sites. In addition to these corrective actions, failure to comply with this policy and procedures may result in disciplinary action up to and including termination.

DEFINITIONS

Credentials. A combination of user name, password, and possibly additional information or keys such as a PIN, biometric scan, or dongle that together are used to access a computer system or information resource.

Data. Alphanumerical or other information represented either in a physical form or digital form suitable for electronic processing or storage.

Encryption. The encoding of data into a form that cannot be easily decoded by unauthorized parties.

Family Educational Rights and Privacy Act of 1974 (FERPA), also known as the Buckley Amendment. FERPA is a federal law that protects the privacy of student academic records.

Gramm-Leach Bliley Act (GLBA). GLBA is a federal law that protects consumers' personal financial information held by financial institutions, including universities.

Health Information Technology for Economic and Clinical Health (HITECH) Act. The HITECH Act promotes the adoption and meaningful use of health information technology. Subtitle D of the HITECH Act addresses privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Health Insurance Portability and Accountability Act of 1996 (HIPAA). HIPAA protects the security of individually-identifiable health information.

Institutional data. All data created, collected, maintained, recorded, or managed by the university, its staff, and agents working on its behalf, in the course of conducting university business.

Internet cloud storage. Data stored in third-party data centers, e.g., CrashPlan, Dropbox, iCloud, Google Drive, OneDrive, Box, etc.

Mobile computing device. Cellular telephones, smartphones, laptop computers, tablets, and similar mobile electronic devices that are capable of storing, processing, displaying, and communicating data.

Network identification (NID). A UCF-issued credential to be used by university employees and students to access enterprise computing systems and applications. The NID, by itself, is classified as restricted data.

Restricted data. Any confidential or personal data that are protected by law or policy and that require the highest level of access control and security protection, both in storage and in transit.

There are two sub-classifications of restricted data

Highly Restricted Data: Examples of highly restricted data are: a) an individual's first name or first initial and last name in combination with any one or more of the following data elements for that individual: social security number, driver's license or identification card number, passport number, military identification number, or other similar number issued on a government document used to verify identity, or financial account numbers; b) user name (e.g., NID) or email address, in combination with a password or security question and answer that would permit access to an online account; c) data concerning an individual that is considered "nonpublic personal information" within the meaning of Title V of the Gramm-Leach Bliley Act of 1999 (Public Law 106-102, 11 Statute 1338) (as amended) and its implementing regulations, and; d) data concerning an individual that is considered "protected health information" within the meaning of the Health Insurance Portability and Accountability Act of 1996 (as amended) and its implementing regulations, and the HITECH Act. Protection of such data may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.

Other examples of highly restricted data include the home addresses, telephone numbers, social security numbers, and photographs of certain university employees, such as police officers and their spouses, as specified in F.S. 119.07(4)(d)1-7.

Unauthorized access to, or disclosure of, highly restricted data will generally require notification to affected parties under the guidelines of state and federal breach notification laws.

Restricted Data: Restricted data include electronic information the unauthorized access, modification, or loss of which could adversely affect the university (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the university), or adversely affect the public.

Examples of restricted data include business-sensitive data, proprietary intellectual property data, and student academic records as defined by the Family Educational Rights and Privacy Act (FERPA) of 1974, and other data protected by law or regulation.

Unauthorized access to or disclosure of certain types of restricted data will generally not require notification of affected parties; however, breach or disclosure of certain restricted data covered by law or regulation may require notification of an appropriate governmental

agency. Unauthorized access to or disclosure of restricted data that are the subject of contractual protections will generally require notification to the contracting party.

Secure sockets layer (SSL)/transport layer security (TLS). Protocols that ensures privacy between communication applications and their users on the Internet.

Strong password. A password that is difficult to guess, consisting of eight (8) or more characters, including lower case and upper case letters, numerals, and special characters. Longer passwords or passphrases are, in general, more secure than shorter passwords. Additional password requirements are contained in the Password Standards document referenced under related documents.

UCFID. UCF-issued identification number that uniquely identifies each university employee and student in the university's administrative systems. The UCFID, by itself, is classified as unrestricted data.

Unrestricted data. Data that are not protected by law or contract, and the disclosure of which would cause no harm to the university or to the affected parties. Examples of unrestricted data include employee names, dates of hire, rate of pay, title, office address, UCFID or phone number. Student names, years, majors, or other directory information not blocked by a student within the scope of FERPA, can be considered unrestricted data.

Virtual private network (VPN). A secure means of connecting to a private network, such as the UCF network, through an insecure network such as the Internet or public wireless network. A VPN connection encrypts data during transmission.

PROCEDURES

The following procedures state general rules relating to the storage, transfer, and access of restricted data. More specific requirements may exist in certain contracts, such as research agreements with the federal government. To the extent specific requirements are set forth in a contract or otherwise required by the government, those specific obligations for storage, transfer, and access of restricted data must be followed.

<u>Highly Restricted Data</u>

- must be stored it in an encrypted form on a secure UCF server, with access protected by a strong password;
- must have full disk encryption using current industry standards if highly restricted data must be stored on desktop workstations in conjunction with official university business processes;
- must never be stored on mobile devices such as laptops, tablets, smartphones, or USB drives;

- may be placed only in a UCF-sanctioned Internet cloud data storage system intended for highly restricted data, but not in personal cloud data storage accounts;
- must not be posted on any public website, blog, or other publicly-accessible Internet site;
- must not be sent via electronic mail, or in an email attachment unless encrypted using current industry standards;
- must not be sent via instant messaging or other unencrypted applications;
- must always be protected by using a secure connection method, such as a VPN and/or SSL/TLS when transmitted through a data network;
- must be stored in a locked cabinet or drawer in a location where access is controlled by a lock or card reader, or that otherwise restricts access to only authorized persons when in hard copy format;
- must not be disclosed to third parties without explicit management authorization and then only on a need-to-know basis;
- must be sent only to a known number when sent via fax;
- must be destroyed when no longer needed, subject to the State of Florida General Records Schedule and UCF policy 4-010.

Restricted Data

- can be stored on workstations or mobile computing devices if the devices are protected by a strong password. File level encryption is required. Full disk encryption is recommended. May be placed only in a UCF-sanctioned Internet cloud data storage system, but not in a personal cloud data storage system;
- may be sent to users who are within a university-provided email system (e.g., UCF Exchange, Knights email, Webcourses@UCF). May be sent to recipients who use external email systems if encrypted using current industry standards;
- instant messaging of restricted data between faculty, staff, and students must be through a university-provided instant messaging system, (i.e., Lync or Skype for Business). Instant messaging may not be used to send restricted data to external systems;
- must not be posted on any public website, blog, or other publicly-accessible Internet site;
- must be sent only to a known number when sending via fax;
- must be destroyed when no longer needed, subject to the State of Florida General Records Schedule and UCF policy 4-010.

Requests for University Data

Court orders, subpoenas, or requests from federal or state agencies for access to university data should be referred to the Office of the General Counsel. All public records requests for university data should be processed according to UCF Policy 2-100.1 *Florida Public Records Act – Scope and Compliance*.

RELATED DOCUMENTS

Policy 2.100.1 - *Florida Public Records Act—Scope and Compliance* policy
Policy 2-103 - *Use of Copyrighted Material policy*

Policy 3-206.1 - *Cardholder Information Security Procedures policy*
Policy 4-007.1 - *Security of Mobile Computing, Data Storage, and Communication Devices policy*
Policy 4-002 - *Use of Information Technologies & Resources Policy*
Policy 4-010 - *Records Management Policy*
Policy 4-209 - *Export Control Policy*
Policy 4-014 - *Procurement and Use of Cloud Computing and Data Storage Services*

Records retention schedule
http://dos.myflorida.com/media/693588/gs05.pdf

UCF password standards
http://www.cst.ucf.edu/wp-content/uploads/501-101-Password-Standards.pdf

How-to guide on encrypting document and files
http://www.cst.ucf.edu/wp-content/uploads/ISO-How-To-508-Encrypting-Files-and-Documents.pdf

Florida Information Protection Act of 2014
http://www.flsenate.gov/Session/Bill/2014/1524#1524

CONTACTS
Computer Services and Telecommunications, Information Security Officer, 407-823-3863

INITIATING AUTHORITY Provost and Executive Vice President

POLICY APPROVAL
(For use by the Office of the President)

Policy Number: 4-008.1

Initiating Authority: Dale Whittaker Date: 8/24/2015

University Policies and Procedures Committee Chair: Rhonda L Bishop Date: 8/21/2015

President or Designee: John C. Hitt Date: 8/27/15